Computers & Security, 16 (1997) 165-171

Subject Index for Volume 15

Abilene Paradox
GSSP (Generally-Accepted System Security Principles): a trip to Abilene 567
Access control
an access control scheme based on Chinese remainder theorem and time stamp concept 73
enforcing legal ownership rights by an access control system 212
object oriented cryptographic facility design: export considerations 507
security classification for documents 55
the information security chain in a company 297
the spook solution - now open for business 17
Addresses
plugging the holes in host-based authentication 661
Attacks
a note on distributed coordinated attacks 103
Audit trail analysis
Cooperating Security Managers: distributed intrusion detection systems 441
Authentication
a simple scheme to make passwords based on one-way functions much harder to crack 171
authenticating passwords over an insecure channel 431
plugging the holes in host-based authentication 661
quantitative authentication and vouching 633
smart card based secure password authentication scheme 231

Ballot's confidentiality
a conventional approach to secret balloting in computer networks 249
BS7790
GSSP (Generally-Accepted System Security Principles): a trip to Abilene 567

CD-ROM
information protection for publishers 209
China
computer security in China 369
Chinese remainder theorem
an access control scheme based on Chinese remainder theorem and time stamp concept 73
Civil rights
enforcing legal ownership rights by an access control system 212
Client servers
the role of information security in corporate governance 477
using RAD tools to develop secure client/server applications 289
COBIT
GSSP (Generally-Accepted System Security Principles): a trip to Abilene 567
COCOM
cryptographic controls - the eternal triangle 576
Code of Practice
information security management: the second generation 281
Communications
electronic communications risk management: a checklist for business managers 377
the information security chain in a company 297
Complexity
quantitative authentication and vouching 633
Computer crime
IT security in Dutch practice 157
Computer networks. See Local area networks (LANs); Networks

0167-4048/97/$17.00 © 1997, Elsevier Science Ltd

Computer security. See Security
Confidentiality
electronic communications risk management: a checklist for business managers 377
Conspiracy attack
cryptanalysis and repair of the multiverifier signature with verifier specification 537
Contingency planning
establishing a network security programme 486
the information security chain in a company 297
Copyright
enforcing legal ownership rights by an access control system 212
establishing Web sites - legal issues and risks 198
Corporate governance
the role of information security in corporate governance 477
Costs
open for business - securely 673
Countermeasures
IT security in Dutch practice 157
Criminal rights
enforcing legal ownership rights by an access control system 212
Cryptography. See Encryption

Data communication networks
message encipherment with minimal expansion and redundancy - doing
better than ISO-10126 627
Data security
GOST 34.10 - a brief overview of Russia's DSA 725
Defamation
establishing Web sites - legal issues and risks 198
Digital signature
a conventional approach to secret balloting in computer networks 249
cryptanalysis and repair of the multiverifier signature with verifier specification 537
GOST 34.10 - a brief overview of Russia's DSA 725
Disaster recovery
establishing a network security programme 486
year 2000 - a real IS security issue 499
Distributed coordinated attacks (DCA)
a note on distributed coordinated attacks 103
Distributed systems
a collision-free secret ballot protocol for computerized general elections 339
open for business - securely 673
quantitative authentication and vouching 633
the information security chain in a company 297
Document security
security classification for documents 55
Dynamic
an access control scheme based on Chinese remainder theorem and time stamp concept 73

EDI
message encipherment with minimal expansion and redundancy - doing better than ISO-10126 627
EDIFACT
message encipherment with minimal expansion and redundancy - doing better than ISO-10126 627
Electricity supply
the information security chain in a company 297
Electromagnetic interference
the information security chain in a company 297
Electronic data interchange (EDI)
security issues in the virtual corporation 471
Electronic mail (e-mail)
a probabilistic flaw in PGP design 39
electronic communications risk management: a checklist for business managers 377
Electronic voting
a conventional approach to secret balloting in computer networks 249
an implementable secure voting scheme 327
E-mail. See Electronic mail (e-mail)
Emergency
the information security chain in a company 297
Encryption
a confidentiality system for ISDN inter-PC high-speed file transfer 141

a conventional approach to secret balloting in computer networks 249
a probabilistic flaw in PGP design 39, 39
a simple scheme to make passwords based on one-way functions much harder to crack 171
achieving interoperable security services in open systems products 27
cryptanalysis and repair of the multiverifier signature with verifier specification 537
cryptographic controls - the eternal triangle 576
GOST 34.10 - a brief overview of Russia's DSA 725
message encipherment with minimal expansion and redundancy - doing better than ISO-10126 627
object oriented cryptographic facility design: export considerations 507
open for business - securely 673
plugging the holes in host-based authentication 661
the information security chain in a company 297

Espionage
the information security chain in a company 297

Exports
cryptographic controls - the eternal triangle 576
object oriented cryptographic facility design: export considerations 507
plugging the holes in host-based authentication 661

File transfer
a confidentiality system for ISDN inter-PC high-speed file transfer 141

Filtering
message encipherment with minimal expansion and redundancy - doing better than ISO-10126 627

Financial services
establishing Web sites - legal issues and risks 198

Fire
the information security chain in a company 297

Forgery
cryptanalysis and repair of the multiverifier signature with verifier specification 537

Fuzzy logic
risk analysis modelling with the use of fuzzy logic 239

Group decision support systems
a conventional approach to secret balloting in computer networks 249

Group-oriented scheme
cryptanalysis and repair of the multiverifier signature with verifier specification 537

GSSP (Generally-Accepted System Security Principles)
GSSP (Generally-Accepted System Security Principles): a trip to Abilene 567

Hacking
electronic communications risk management: a checklist for business managers 377

Hash function
GOST 34.10 - a brief overview of Russia's DSA 725

Hypertext
a security officer's workbench 695

Imports
cryptographic controls - the eternal triangle 576

Information security
information protection for publishers 209
information security management: the second generation 281

IT security in Dutch practice 157
risk analysis modelling with the use of fuzzy logic 239
the information security chain in a company 297
the role of information security in corporate governance 477

Information warfare
information warfare - your company needs you 561

Intellectual property
establishing Web sites - legal issues and risks 198

Internet
electronic communications risk management: a checklist for business managers 377
establishing Web sites - legal issues and risks 198

Internet as a pornotopia 203
message encipherment with minimal expansion and redundancy - doing better than ISO-10126 627
open for business - securely 673
the role of information security in corporate governance 477
Intranet
the role of information security in corporate governance 477
Intrusion detection
Cooperating Security Managers: distributed intrusion detection systems 441
IPsec
plugging the holes in host-based authentication 661
ISDN
a confidentiality system for ISDN inter-PC high-speed file transfer 141
ISO 9000
information security management: the second generation 281

Key distribution
a confidentiality system for ISDN inter-PC high-speed file transfer 141
Key escrow
cryptographic controls - the eternal triangle 576
object oriented cryptographic facility design: export considerations 507
Key-lock-pair
an access control scheme based on Chinese remainder theorem and time stamp concept 73
Key management
a confidentiality system for ISDN inter-PC high-speed file transfer 141

Legal issues
enforcing legal ownership rights by an access control system 212
establishing Web sites - legal issues and risks 198
year 2000 - a real IS security issue 499
Local area networks (LANs)
an implementable secure voting scheme 327
the new face of the virus threat 13

Locks
the information security chain in a company 297

Management
information security management: the second generation 281
Medical records
medical records security 100
Message encipherment
message encipherment with minimal expansion and redundancy - doing better than ISO-10126 627
Mobile computing
the information security chain in a company 297
Networks
a conventional approach to secret balloting in computer networks 249
Cooperating Security Managers: distributed intrusion detection systems 441
establishing a network security programme 486
message encipherment with minimal expansion and redundancy - doing better than ISO-10126 627
plugging the holes in host-based authentication 661
using RAD tools to develop secure client/server applications 289

Object classification
security classification for documents 55
Object orientation
object oriented cryptographic facility design: export considerations 507
OECD
GSSP (Generally-Accepted System Security Principles): a trip to Abilene 567
One-way function
a simple scheme to make passwords based on one-way functions much harder to crack 171
authenticating passwords over an insecure channel 431
Open systems
achieving interoperable security services in open systems products 27
open for business - securely 673

Ownership rights
enforcing legal ownership rights by an access control system 212

Passwords
a simple scheme to make passwords based on one-way functions much harder to crack 171
authenticating passwords over an insecure channel 431
plugging the holes in host-based authentication 661
smart card based secure password authentication scheme 231
the information security chain in a company 297
Personal computers
a confidentiality system for ISDN inter-PC high-speed file transfer 141
Personnel
the information security chain in a company 297
PGP
a probabilistic flaw in PGP design 39
Politics
plugging the holes in host-based authentication 661
quantitative authentication and vouching 633
Pornography
Internet as a pornotopia 203
Portability
object oriented cryptographic facility design: export considerations 507
Privacy
a collision-free secret ballot protocol for computerized general elections 339
a confidentiality system for ISDN inter-PC high-speed file transfer 141
electronic communications risk management: a checklist for business managers 377
Private key systems
achieving interoperable security services in open systems products 27
Protection
extending the Schematic Protection Model -II. Revocation 525
information protection for publishers 209
IT security in Dutch practice 157
the information security chain in a company 297
Pseudo-random number generators (PRNG)
a probabilistic flaw in PGP design 39
Public key systems
a probabilistic flaw in PGP design 39
achieving interoperable security services in open systems products 27
open for business - securely 673
smart card based secure password authentication scheme 231
Publishers
information protection for publishers 209

RAD (rapid application development) environments
using RAD tools to develop secure client/server applications 289
RDBMS
using RAD tools to develop secure client/server applications 289
Recovery
the information security chain in a company 297
Regulations
computer security in China 369
Rescue
the information security chain in a company 297
Revocation
extending the Schematic Protection Model -II. Revocation 525
Risk analysis
a security officer's workbench 695
risk analysis modelling with the use of fuzzy logic 239
Risk Data Repository
a security officer's workbench 695
Risk management
electronic communications risk management: a checklist for business managers 377
establishing a network security programme 486
Risk model
a security officer's workbench 695
Risks
establishing Web sites - legal issues and risks 198
the information security chain in a company 297

Russia
GOST 34.10 - a brief overview of Russia's DSA 725

Sabotage
the information security chain in a company 297
Safety
extending the Schematic Protection Model -II. Revocation 525
SALSA
SALSA: a method for developing the enterprise security architecture and strategy 501
Schematic Protection Model (SPM)
extending the Schematic Protection Model -II. Revocation 525
Secret ballot protocols
a collision-free secret ballot protocol for computerized general elections 339
Secret sharing schemes
an implementable secure voting scheme 327
Security
a collision-free secret ballot protocol for computerized general elections 339
a confidentiality system for ISDN inter-PC high-speed file transfer 141
a security officer's workbench 695
a simple scheme to make passwords based on one-way functions much harder to crack 171
achieving interoperable security services in open systems products 27
an implementable secure voting scheme 327
computer security in China 369
establishing a network security programme 486
GSSP (Generally-Accepted System Security Principles): a trip to Abilene 567
medical records security 100
open for business - securely 673
SALSA: a method for developing the enterprise security architecture and strategy 501
security issues in the virtual corporation 471
the information security chain in a company 297
the role of information security in corporate governance 477
the spook solution - now open for business 17
year 2000 - a real IS security issue 499
see also Information security
Self-evaluation
information security management: the second generation 281
Signature
smart card based secure password authentication scheme 231
Smart cards
authenticating passwords over an insecure channel 431
smart card based secure password authentication scheme 231
Social acceptance
a conventional approach to secret balloting in computer networks 249
SOS TDP
achieving interoperable security services in open systems products 27
Spoofing
cryptanalysis and repair of the multiverifier signature with verifier specification 537
SQL
using RAD tools to develop secure client/server applications 289
SSH
plugging the holes in host-based authentication 661
SSL (Secure Sockets Layer)
plugging the holes in host-based authentication 661
Standards
achieving interoperable security services in open systems products 27
GOST 34.10 - a brief overview of Russia's DSA 725
GSSP (Generally-Accepted System Security Principles): a trip to Abilene 567
information security management: the second generation 281
Strategy
SALSA: a method for developing the enterprise security architecture and strategy 501

Theft
the information security chain in a company 297

Threats
IT security in Dutch practice 157
open for business - securely 673
the information security chain in a company 297
Time stamp
an access control scheme based on Chinese remainder theorem and time stamp concept 73
Tools
a security officer's workbench 695

Uniquely blind signature schemes
a collision-free secret ballot protocol for computerized general elections 339
United State
plugging the holes in host-based authentication 661
User IDs
plugging the holes in host-based authentication 661

Verification
cryptanalysis and repair of the multiverifier signature with verifier specification 537
Virtual corporation
security issues in the virtual corporation 471
Virtual Private Networking (VPN)
open for business - securely 673
Viruses
the information security chain in a company 297
the new face of the virus threat 13
Vouching
quantitative authentication and vouching 633

Water damage
the information security chain in a company 297
Web sites
establishing Web sites - legal issues and risks 198

XDSF
open for business - securely 673

Year 2000
year 2000 - a real IS security issue 499

Computers & Security, 16 (1997) 172

Author Index for Volume 15

Adams, D., 673
Anderson, M., 633

Blatchford, C., 203
Bontchev, V., 595
Born, E., 212
Borrell, J., 327
Buckwell, M., 17

Calvelli, C., 525
Chang, J-F., 231
Clark, A., 576
Cohen, F.B., 103, 707

David, J., 13
de Ru., W.G., 239

Eloff, J.H.P., 55, 239
Evans, P., 209

Finne, T., 297
Frank, B., 471

Heinlein, E.B., 100, 369, 499
Holbein, R., 55
Hwang, J-J., 249
Hwang, M-S., 73

Jansen, C., 627
Juang, W-S., 339

Kovacich, G., 486
Krull, A., 567
Kwok , L.F., 695

Lei, C-L., 339
Lemieux, J., 289
Lindup, K., 477
Longley, D., 695
Looijen, M., 157

Manber, U., 171
Matsumoto, H., 141
Michels, M., 725
Miller N., 198
Moreau, T., 39
Moulton, M.E., 377
Moulton, R.T., 377

Naccache, D., 725

Oyaizu, I., 141

Petersen, H., 725
Porter, T., 561
Press, J., 507

Reid, J., 661
Rifà, J., 327

Sherwood, J., 501
Smith, P., 27
Spruit, M., 157
Sung, H-S., 431
Teufel, S., 55
Tzeng, W-G., 73

van der Vlist, P., 627
Varadharajan, V., 525
von Solms R., 281

Wang, S-J., 231
White, G., 441
Wu, T-C., 431

Yang, W-P., 73
Yen, S-M., 537
Yesberg, J., 633